PWNBOXER

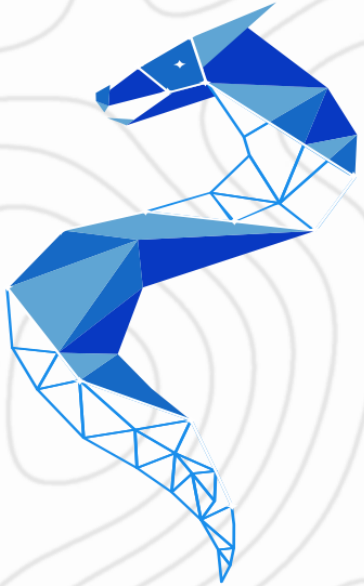
Group 22

Franco Mezzarapa

Robert Lee

Abdiel Marcano

Gugulethu Sigogo



Advisor: Dr. Saleem Sahawneh | Committee: Dr. Mike Borowczak, Dr. Nazanin Rahnavard, Dr. Justin Phelps

TEAM

Franco Mezzarapa
- Computer Engineer -

Robert Lee
- Computer Engineer -

Abdiel Marcano
- Computer Engineer -

Gugulethu Sigogo
- Electrical Engineer -

MOTIVATION

Cyberthreats evolve every day.	Threat actors target corporations and people.
	New Exploits found often.
Penetration Testing is expensive	Contracting penetration test is expensive - $2,000 - $50,000
	Automated testing tools are not available to general consumers.
Self-testing is difficult.	Requires ability to perform testing
	Tooling output is still difficult to interpret.

GOALS

Basic Goals

- Portable, automated network auditing and vulnerability detecting device
- Generate vulnerability reports
- MCU → CM4 data transfer
- CM4 runs network security scans and processing
- LED indicators and Display for system condition feedback
- Direct technician or developer access through external peripherals
- Provide a web portal for users to upload, view, and download generated reports

Advanced Goals

- Customizable audit durations
- Simultaneous auditing of multiple networks
- Technician-defined vulnerability tests

Stretch Goals

- Animated audit progress indicators
- Integration with external AI provider (LLM evolution path)
- Advanced dashboard analytics

OBJECTIVES

Basic Objectives

- Generate vulnerability reports using LLM
- Execute Nmap/Nessus
- Touchscreen interface
- LEDs
- Deliver generated reports via web portal and send via email

Advanced Objectives

- Remote technician support
- UART comm MCU ↔ CM4
- Concurrent audits

Stretch Objectives

- Develop advanced reporting dashboard with historical analytics and trends
- Integrate an onboard audio alert system for audible notifications for key operational events
- Add API-based integration to support custom vulnerability tests

ENGINEERING SPECIFICATIONS

Maximum Audit Completion Time	4 Hours
Maximum Power Consumption	15W
Onboard Data Storage	32GB eMMC + 4MB SPI Flash
Onboard Memory Size	8GB LPDDR4 + 512KB SRAM
Weight	2 lbs.
Size	13.35 cm Diagonally
Display	3.5″ TFT with Touch
AI Model	Qwen2.5 - 7b

WEB SYSTEM ARCHITECTURE

Clients

User (Browser)
- Login / Upload / View Reports
- Admin Access

PwnBoxer Device (CM4)
- Runs scans
- Uploads artifacts via API key

HTTPS

Authenticated API upload

Application Layer

Next.js Frontend (UI Layer)
- Dashboard + Uploads
- Sends REST requests

NEXT.js

REST API + JWT (Bearer)

Node/Express Backend (API Layer)
- JWT auth + role checks
- Device API key auth
- Handles uploads + report lifecycle
- Streams downloads

node js express

Prisma ORM Queries

Read/Write Reports & Uploads

LLM inference request (local service)

Data & AI Layer

PostgreSQL Database
- Users, API keys, reports, uploads

docker

File Storage (Disk)
- Artifacts + generated reports

Qwen LLM (Report Generator)
- Reads scan artifacts
- Generates vulnerability report
- Backend stores output

Qwen

WEB SOFTWARE DESIGN - BACKEND

- REST API Architecture (Node.js + Express)
- JWT-based authentication (stateless)
- Role-based access control (user vs admin)
- Device authentication via API keys (prefix + hashed secret)
- Report lifecycle state machine (pending → completed / failed)
- Prisma ORM for PostgreSQL interaction
- File handling via Multer (multipart uploads)

ADMINISTRATION & DEVICE MANAGEMENT

Admin Capabilities

- Generate and revoke API keys
- Assign devices to users
- Track device activity and last upload
- Disable compromised devices

Security Benefits

- Revocable credentials limit breach impact
- Device attribution for each report
- Role-based admin controls

AUTHENTICATION & AUTHORIZATION

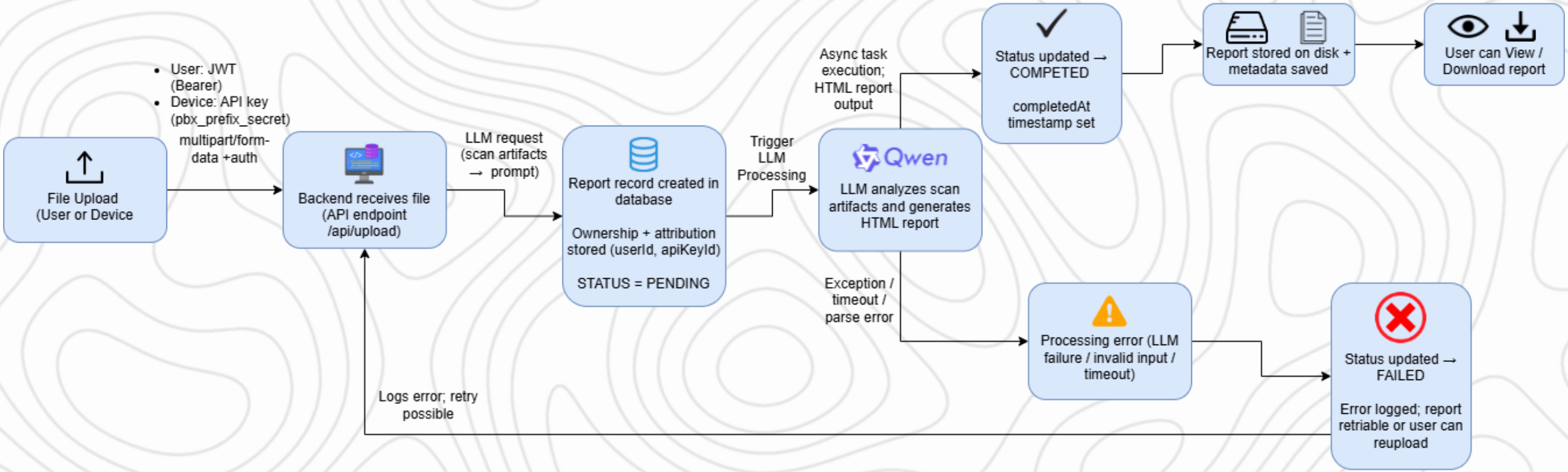
Human Authentication

- User enters username + password
- Password checked against encrypted hash (bcrypt)
- System issues secure login token (JWT)
- Token used to access dashboard and reports and future requests

Device Authentication

- Admin generates API key
- Key stored securely (hashed)
- Device uploads using: Bearer pbx_prefix_secret
- Backend verifies device identity
- Upload linked to correct user + device

REPORT LIFECYCLE



WEB SYSTEM CONSTRAINTS & ASSUMPTIONS

- Email delivery requires internet connectivity
- Audit duration varies with network size and scan depth
- Local LLM processing time depends on compute resources
- Device uploads require valid API key authentication
- Concurrent audits limited by CM4 CPU and memory capacity

PWNBOXER

LIBRARY SELECTION – DISPLAY DRIVER

Metric	TFT_eSPI	LovyanGFX	Custom
Description	Arduino based library for controlling TFT displays.	C++ Library for driving various displays	C library for driving the ILI9488 TFT panel.
Advantage	• Simple library use. • Fast prototyping • Preconfigured header file for different microcontrollers	• DMA support for both SPI and Parallel • Not dependent on Arduino. • Touch library included.	• No dependencies • Tailored to microcontroller in use. • Potentially less overhead.
Disadvantage	• Limited DMA support for ESP32-S3, no parallel DMA support	• Moderate complexity implementation	• Requires in-depth LCD peripheral knowledge

LIBRARY SELECTION – RENDERING LIBRARY

Metric	LVGL
Description	Hardware agnostic GUI library.
Advantage	• Rich widget/theme options. • Simple widget deployment.
Disadvantage	• Moderate integration difficulty through callback functions. • Functions are not wrapped in a class.

PWNBOXER

SOFTWARE SELECTION – VULNERABILITY ASSESSMENT TOOLS

Metric	NMAP	Metasploit Framework	Nessus Vulnerability scanner
Description	Network scanner used for detection of active services.	Framework used for vulnerability scanning, and active testing.	Network and service vulnerability detection.
Advantage	• Supports a variety of scan options. • Built in scripting engine. • Accuracy with service detection, OS detection.	• Includes a large repository of testing modules. • Added functionality through ruby modules	• Provides authenticated scanning for hosts. • Provides detailed reporting output. • Adequate false positive rate
Disadvantage	• Can be slow on resource constrained devices.	• Requires more configuration to run modules.	• Resource heavy for large host ranges.

SOFTWARE SELECTION – TECHNICIAN CONNECTIVITY

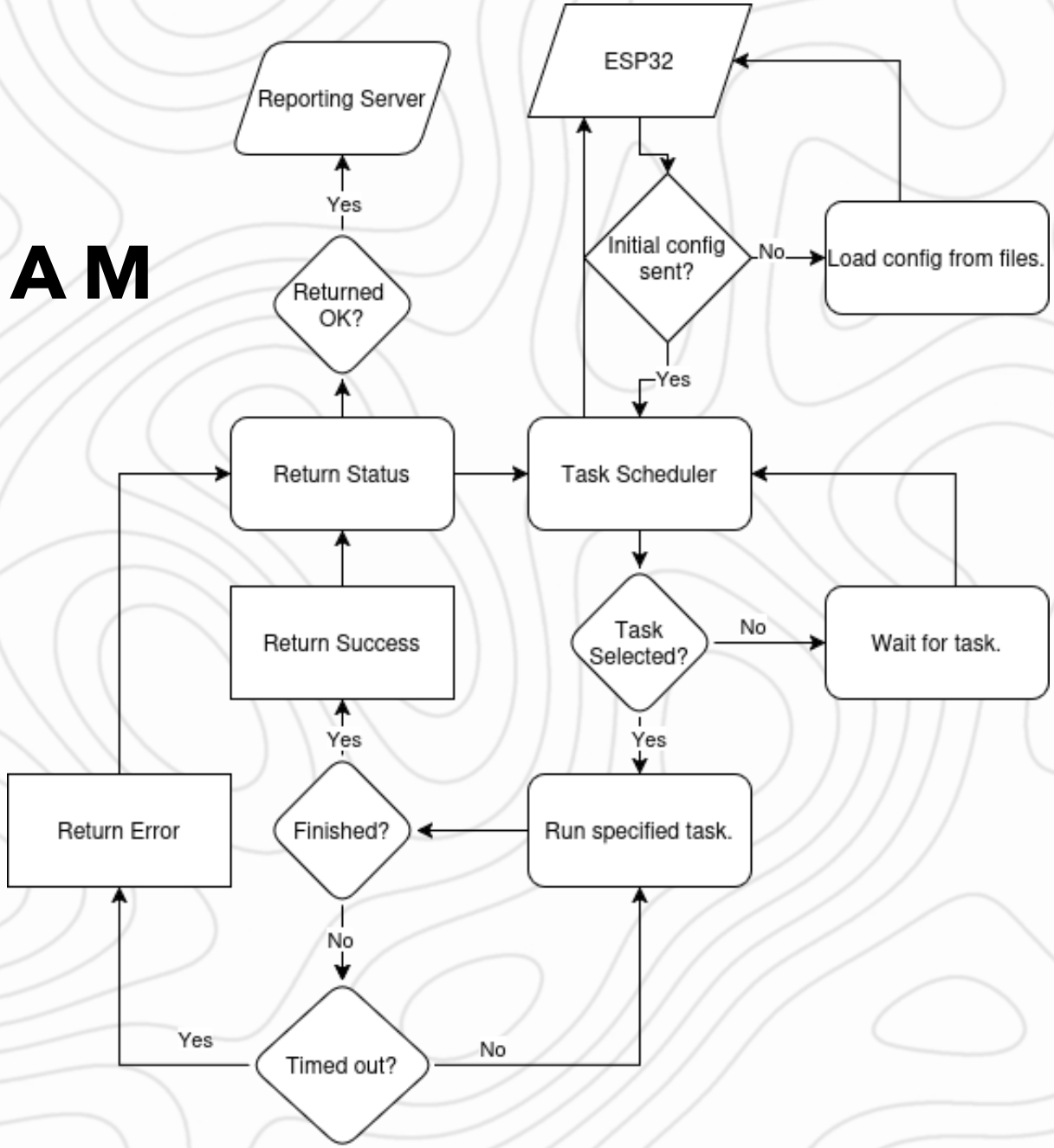
Metric	Meterpreter	Sliver	Netcat
Description	Metasploit built in beacon/session payloads.	Command and Control beacon/session payloads.	Command line utility for reading and writing network data.
Advantage	• Built into Metasploit through MSFVenom • Additional auditing modules can be run in shell. • Fast compile times.	• MTLS connection allowing authenticated and encrypted traffic. • Multiplayer Sessions • BOF support.	• No dependencies • Lightweight for embedded systems use. • Built into most Linux distributions.
Disadvantage	• No authentication, or DNS support.	• Long compile time for beacons.	• Limited interactive shell capabilities.

FIRMWARE DIAGRAM

- On boot, the ESP32 checks if initialization has completed.
  - If not, it starts peripherals, loads config from flash, and reconnects to previously detected WiFi networks.
- The ESP32 and CM4 exchange data over UART.
  - Credentials and settings are sent to the CM4, which returns a list of available tasks.
- Once synchronized, the display shows available tasks and current settings and waits for user input.
- Setting changes are saved to flash and re-sent to the CM4.
- Task selections are forwarded to the CM4 and the ESP32 begins polling for status.
- On task completion, a success or error message is shown and the user is prompted to confirm before returning to the main display.

SCHEDULER DIAGRAM

- On boot, the scheduling software starts as a system service and checks whether the initial configuration has been set.
  - If not, it loads from local files and sends the ESP32 the relevant task information.
- Once configured, the scheduler waits for an incoming task from the ESP32.
- When a task is received, the scheduler pulls its parameters from the task's config file, starts execution, and begins a timer to monitor progress.
- If the task exceeds the timeout, it is terminated and a timeout error code is returned. If it crashes, a failure error code is returned. If it completes successfully, a completion code is returned.
- All result codes are sent back to the ESP32 for display on screen.

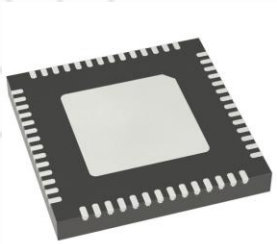


SBC COMPARISON AND SELECTION

Feature	BeagleBone AI-64	Raspberry Pi CM4	Raspberry Pi CM5	NVIDIA Jetson Nano
Operating Voltage	5V	5V	5V	5V
RAM	4GB	8GB	8GB	4GB
eMMC	16GB	32GB	32GB	16GB
Wi-Fi	No	Yes	Yes	No
Cost	$185	$125	$156	$129

MCU COMPARISON AND SELECTION

Feature	ESP32-WROOM-32	ESP32-S3	MSP430	STM32
No. of GPIO	26	45	83	37
Operating Voltage	3.0-3.6V	3.0-3.6V	1.8-3.6V	2.0-3.6V
IDE	VSCode/PlatformIO	VSCode/PlatformIO	CCS	STM32CubeIDE
Cost	$5	$6	$11	$4

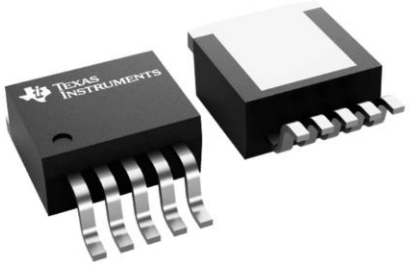


REGULATOR COMPARISON

Specifications	Linear Regulator	Switching Regulator
Cost	Low cost; inexpensive components and simple design	Higher cost; requires more components (inductor, diode, capacitor, switch)
Efficiency	Low (typically 30–60%); energy lost as heat	High (typically 80–95%); minimal energy wasted
Heat	Generates significant heat due to voltage drop across pass transistor	Much cooler operation due to efficient power conversion
Voltage Output (relative to input)	Can only step down	Can step up, step down, or invert voltage
Complexity	Simple design and easy to implement	Complex design; requires careful layout and EMI considerations

REGULATOR SELECTION

Feature	LM2576SX-ADJ/NOPB
Input Voltage	Up to 40V
Output Voltages	Adjustable, using 3.3V and 5V
Max Output Current	3A
Cost	$3

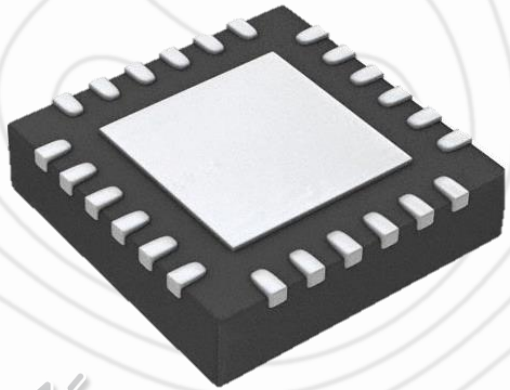


DISPLAY COMPARISON AND SELECTION

Specification	CFAF320480C7-035TC	NHD-1.8-128160EF-SSXN-FT	CH700WV03A-T
Size (in)	3.5	1.8	7.0
Cost (USD)	~ $35	~ $20	~ $60
Contrast Ratio	1000:1	500:1	500:1
Luminance (cd/m^2)	300	300	280
Resolution (pixels)	320 × 480	128 × 160	800 × 480
Interface	8/9/16/18-bit Parallel, I^{2}C (Touch)	3/4-wire SPI	40-pin 24-bit Parallel
Supply Voltage (V)	3.3	3.0–3.3	3.3
Touch Type	Capacitive	Resistive	Resistive

PD SELECTION

Feature	STUSB4500	IP2721-MAX12	FUSB302B
Voltage Profiles	Up to 20V	5 / 9 / 12 V	Up to 28V
Unit Price	$1.94	$1.04	$1.58
Flexibility	High	Low	High
Setup Complexity	Medium	Low	High

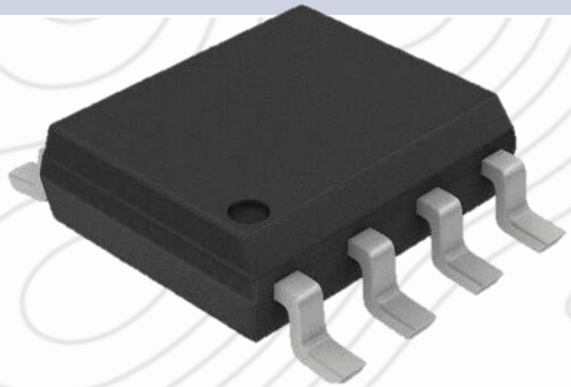


USB-TO-UART SELECTION

Feature	CP2102
USB Standard Support	USN 2.0 Full- Speed compliant
Availability	High
Integration Complexity	Low
High Volume of Documentation	

FLASH MEMORY SELECTION

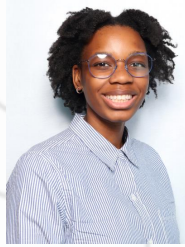
Feature	W25Q32JV
Interface	SPI
Storage	4MB SPI
Integration Complexity	Low
Industry Adoption	Very High
Cost	$0.93



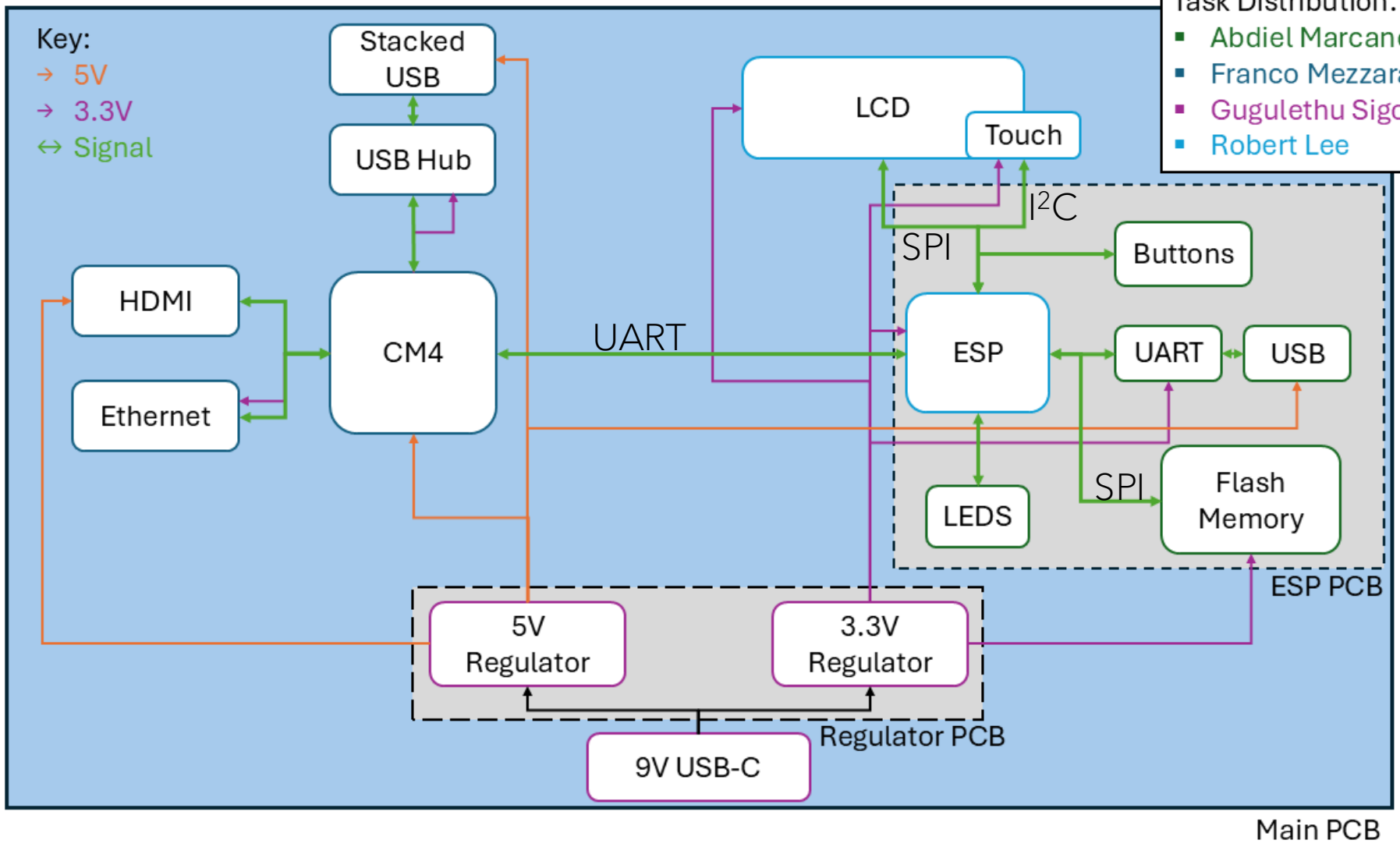
USB HUB SELECTION

IC	USB Generation	HID Suitability	Configuration	Integration Complexity	Cost
USB2512B	USB 2.0 Hi-Speed	✓	Strap	Low	$2.38
TUSB8020B	USB 3.0	✓	Strap + EEPROM + SS config	High	$10.30
CY7C65620	USB 2.0 Hi-Speed	✓	EEPROM/GPIO configurable	Medium	$15.30

HARDWARE BLOCK DIAGRAM



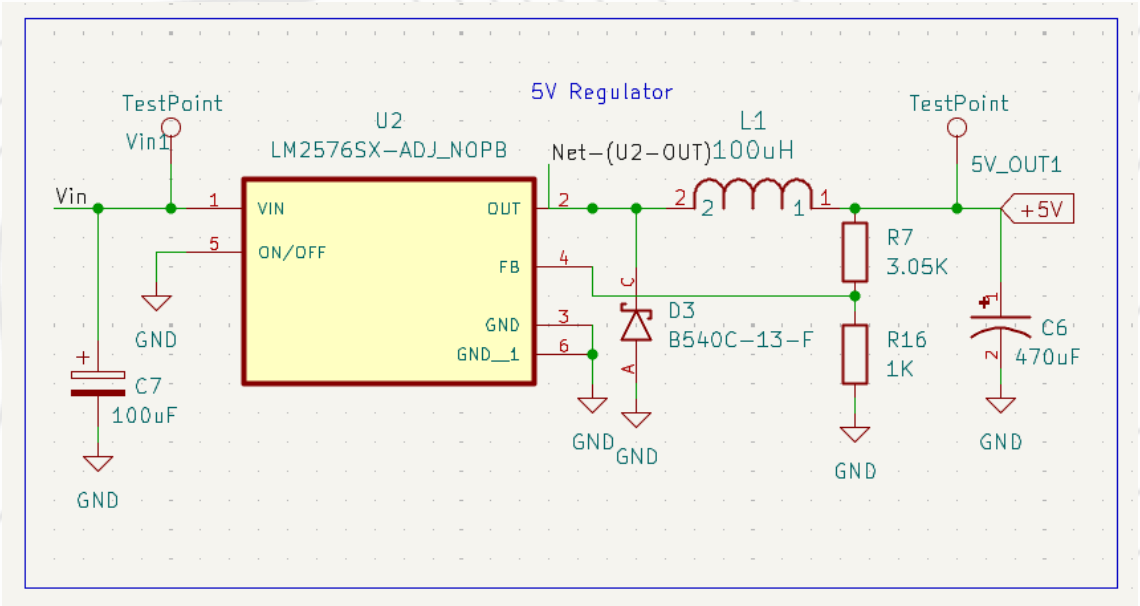
Task Distribution:
- Abdiel Marcano
- Franco Mezzarapa
- Gugulethu Sigogo
- Robert Lee

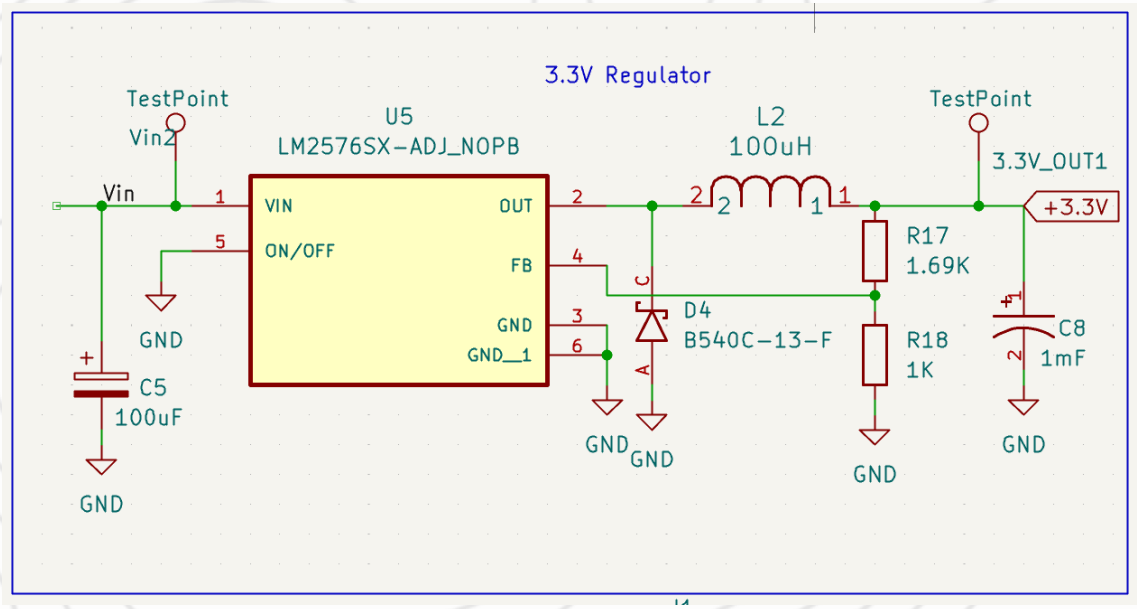


PWNBOXER

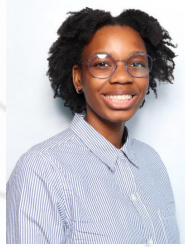
REGULATOR SCHEMATICS

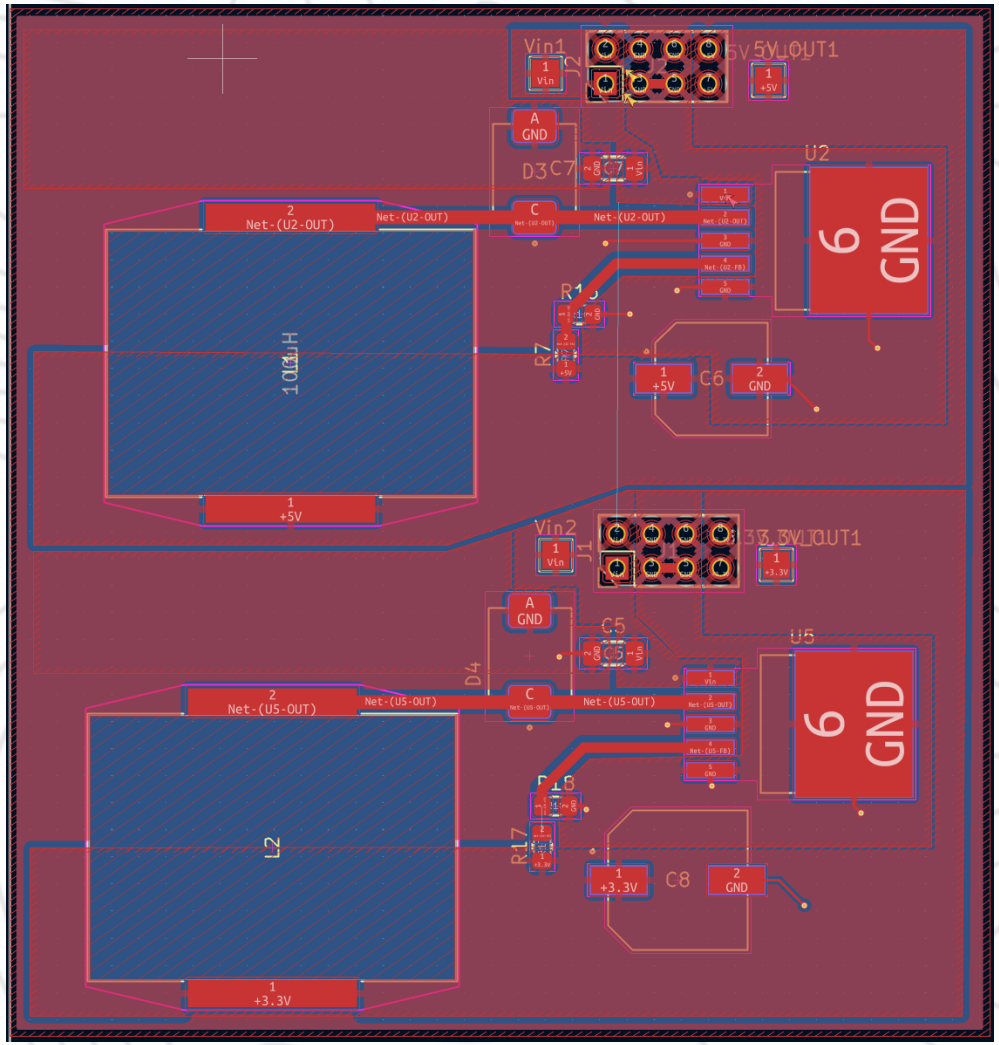
5V & 3.3V Switching Regulators



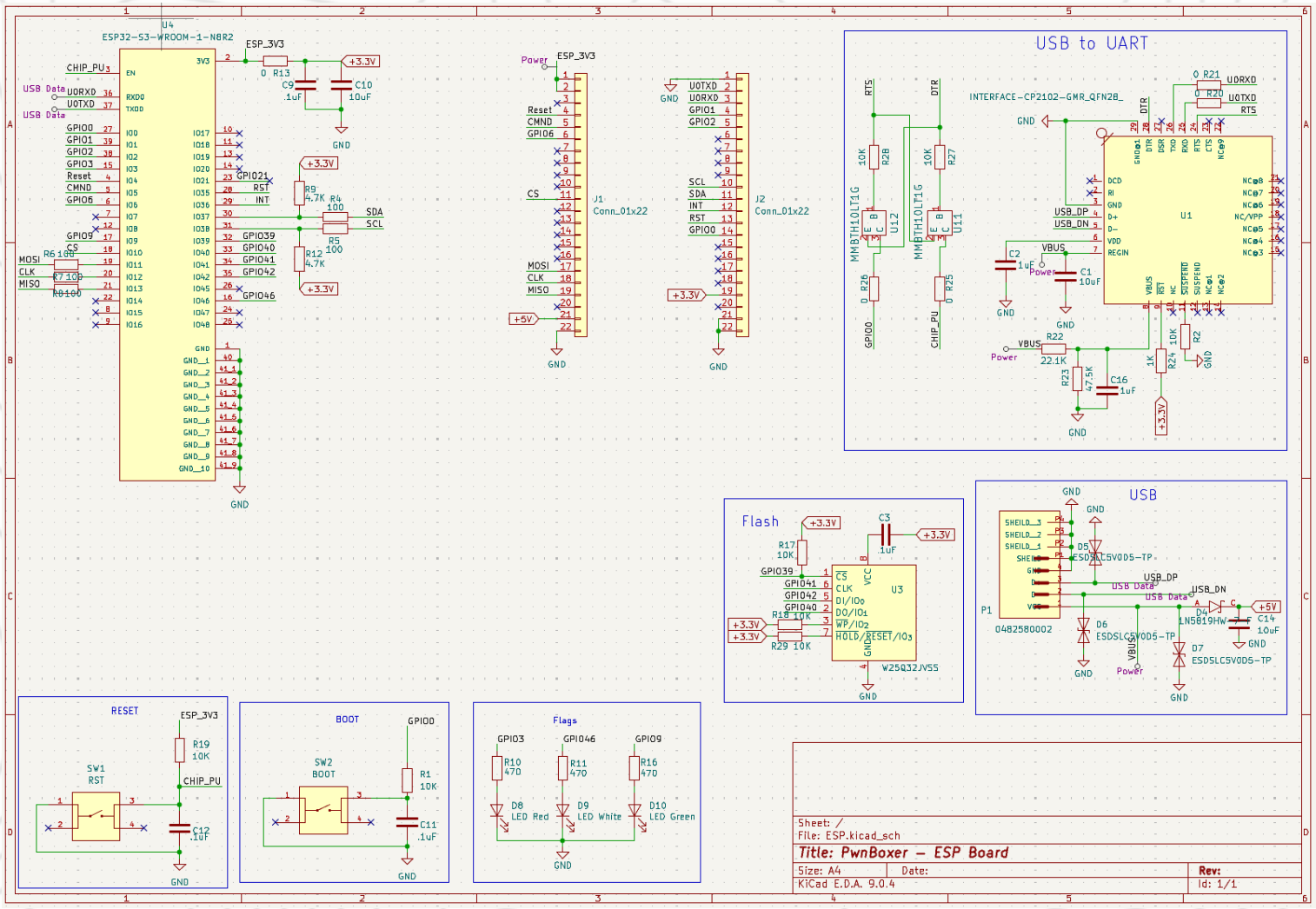


REGULATOR PCB DESIGN

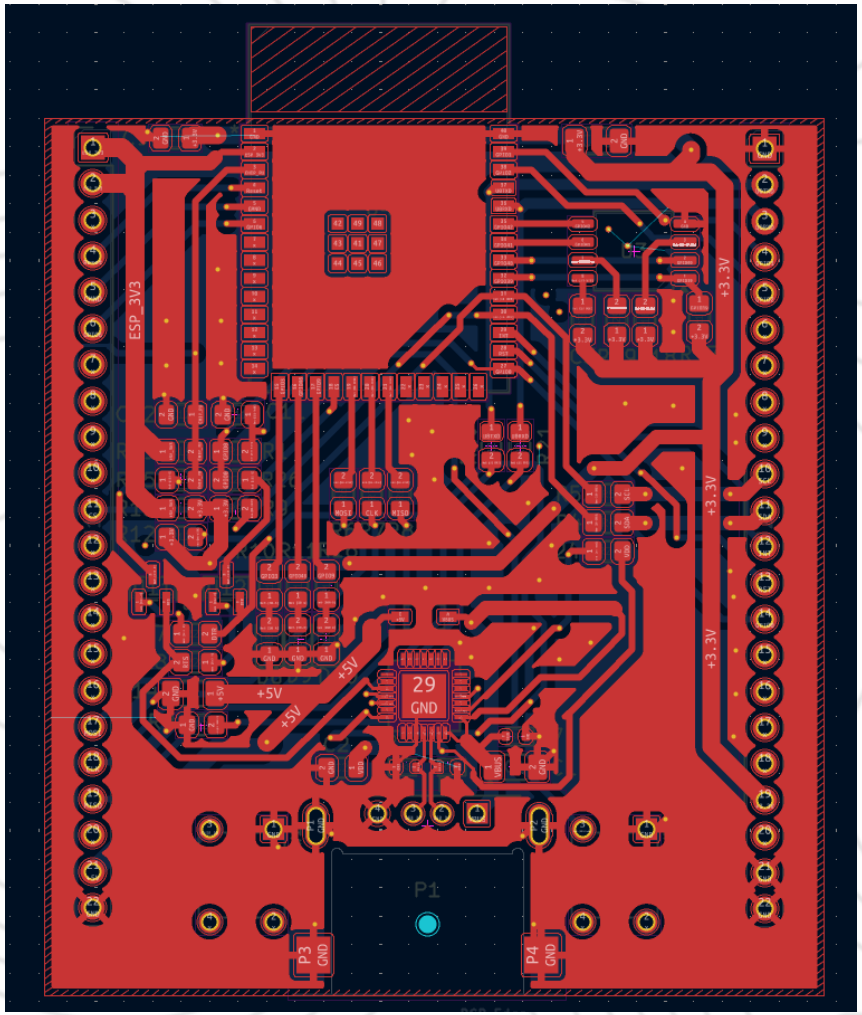


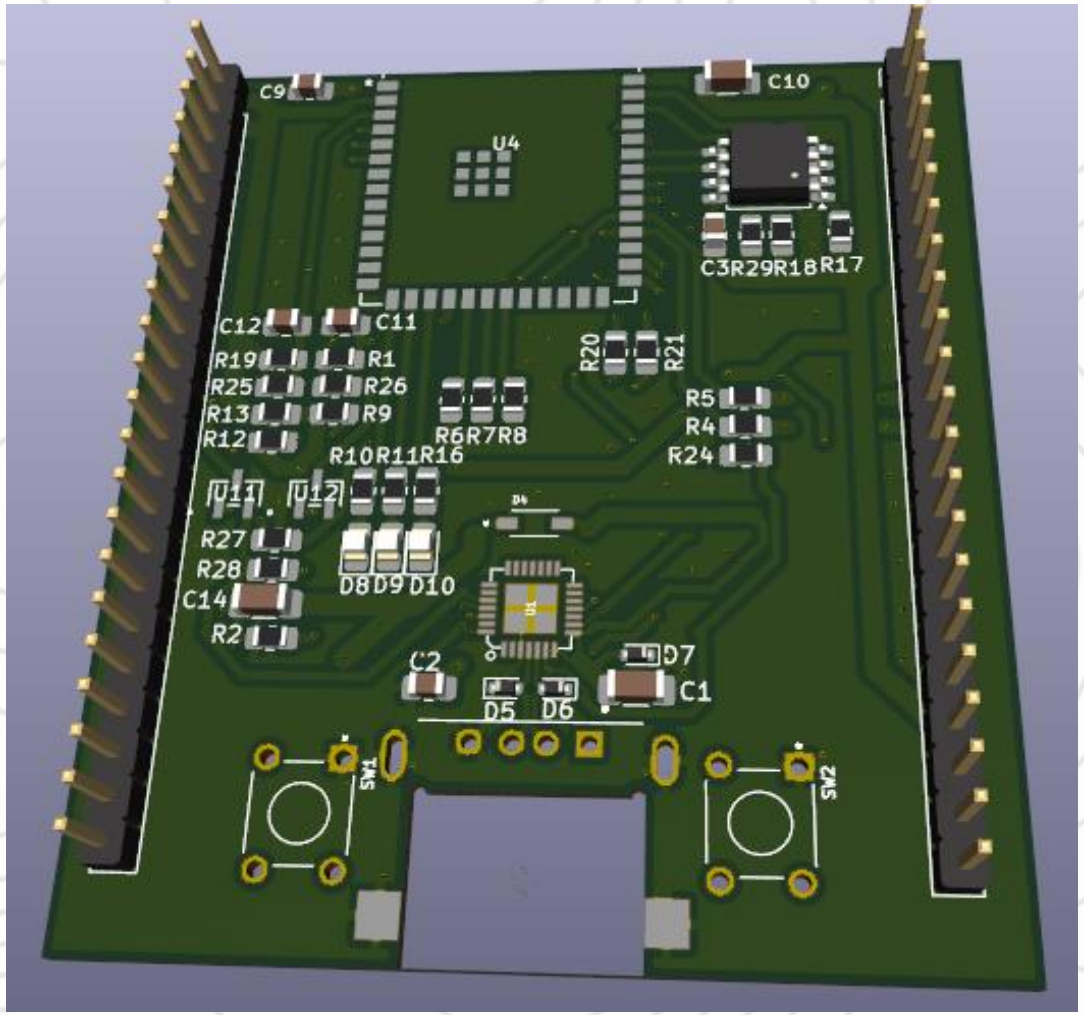


ESP32 SCHEMATIC



ESP32 PCB DESIGN

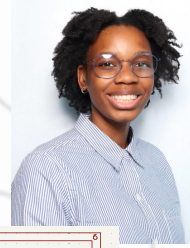


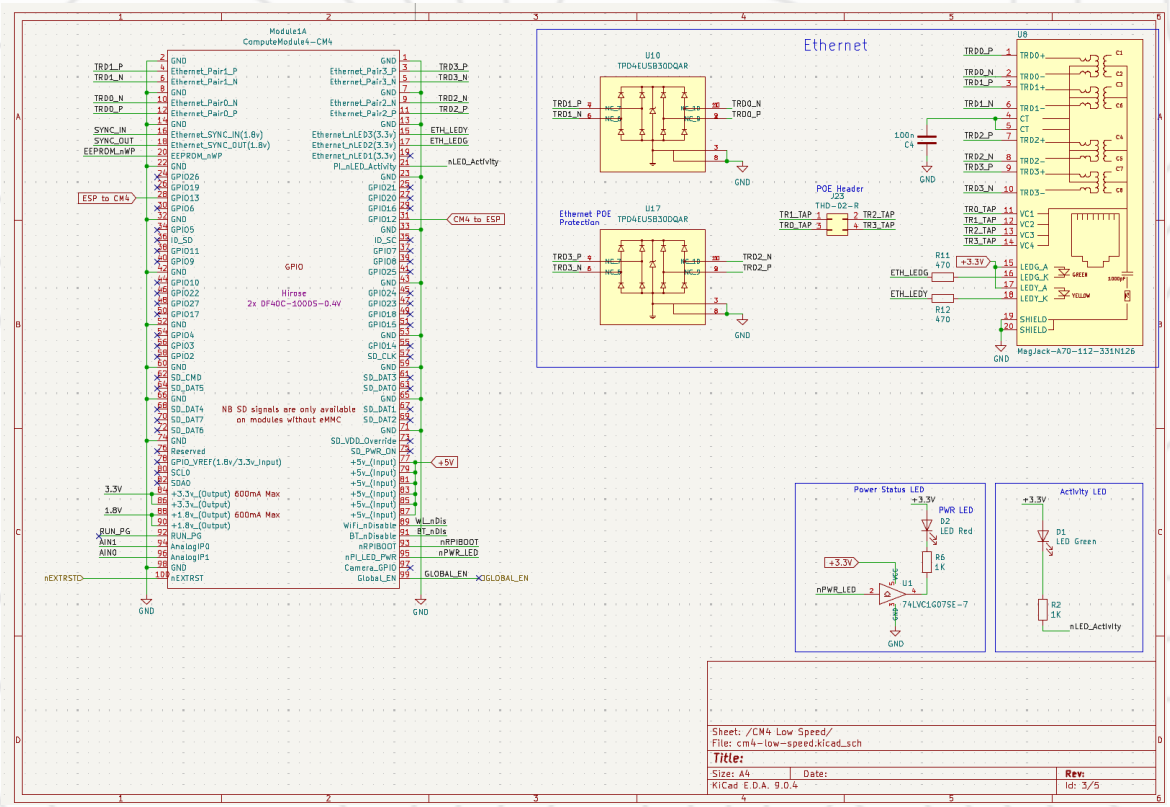


PWNBOXER

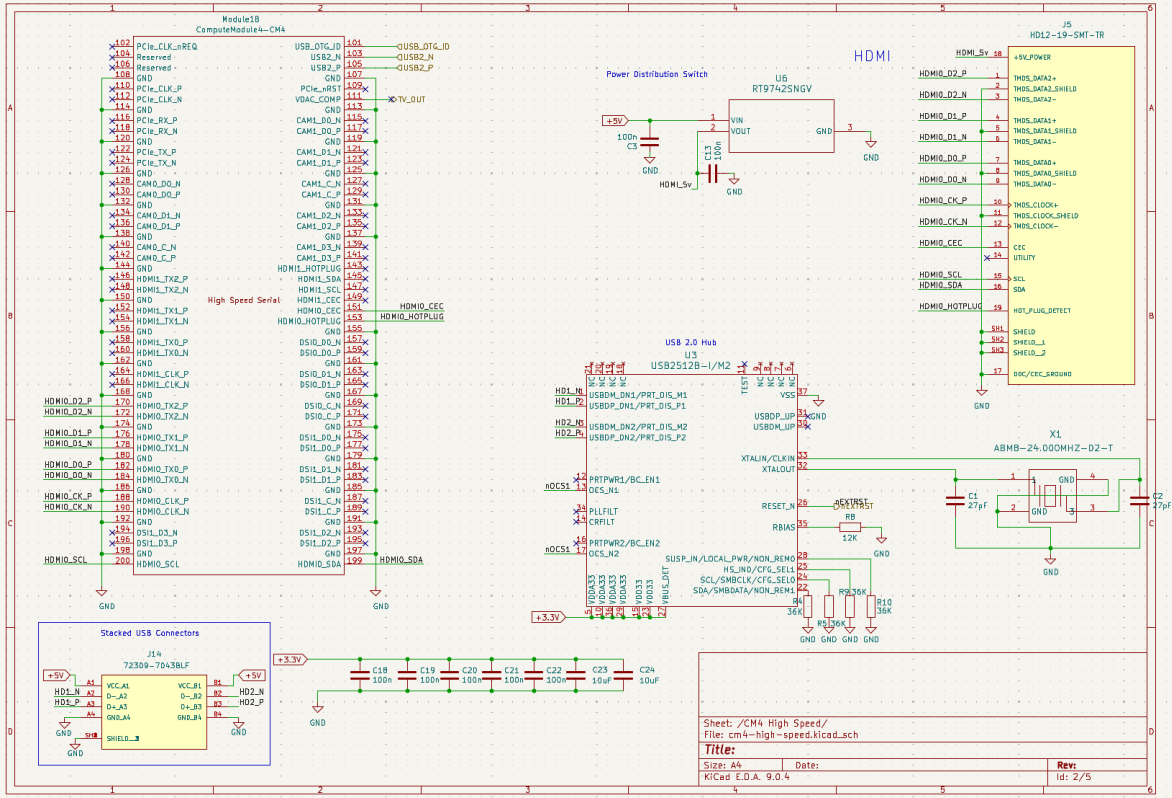
MAIN BOARD SCHEMATIC

CM4 HEADE4RS





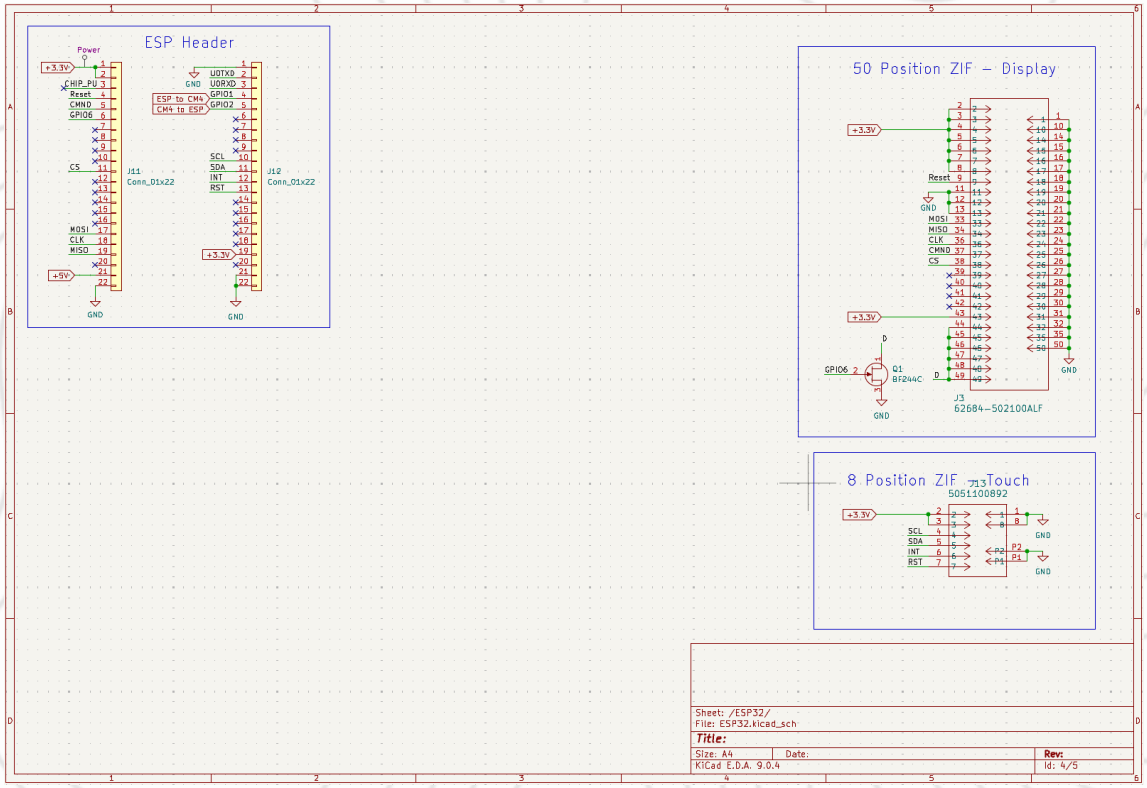
Low Speed



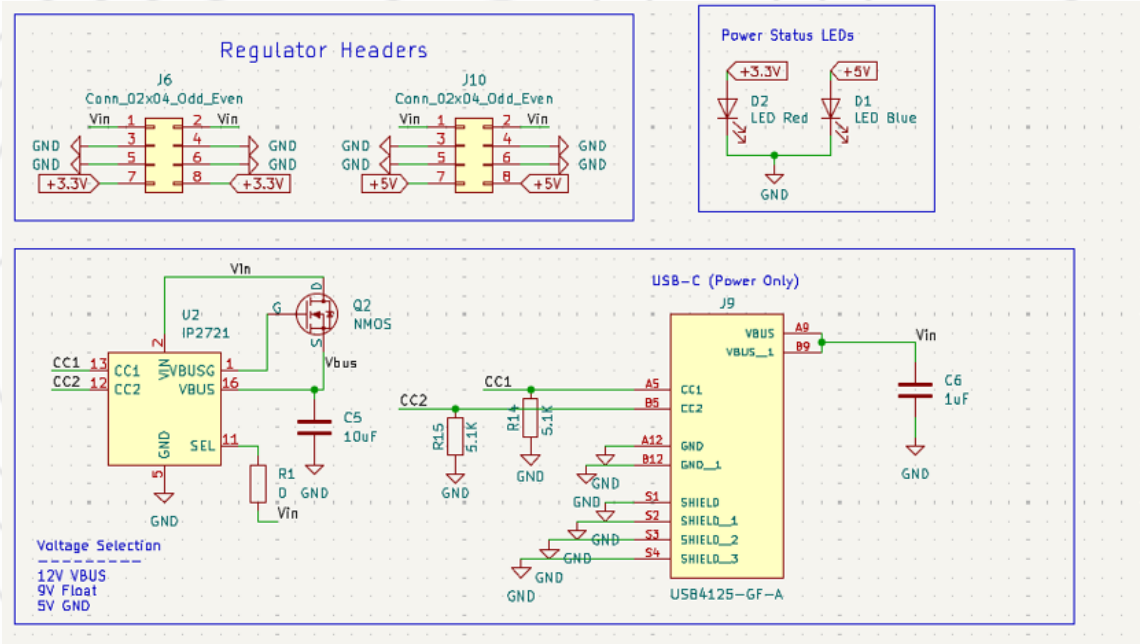
High Speed

PWNBOXER

MAIN BOARD SCHEMATIC

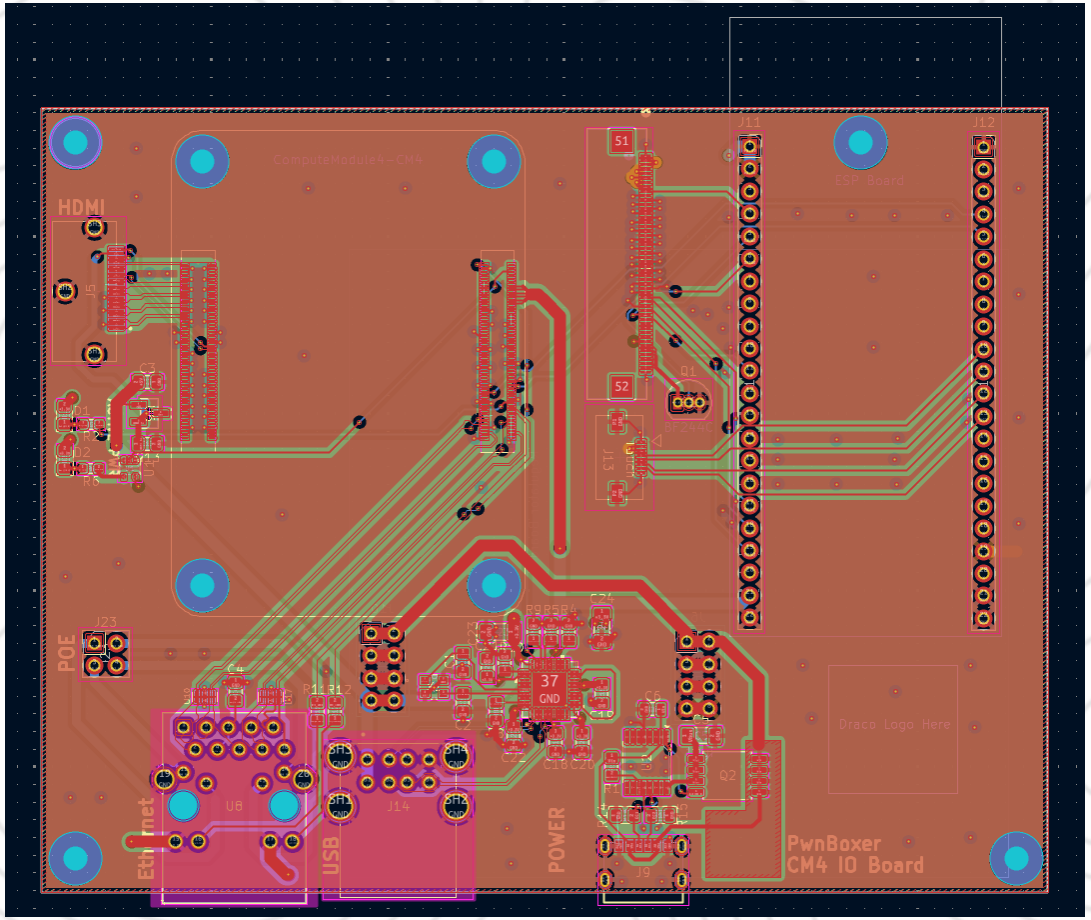


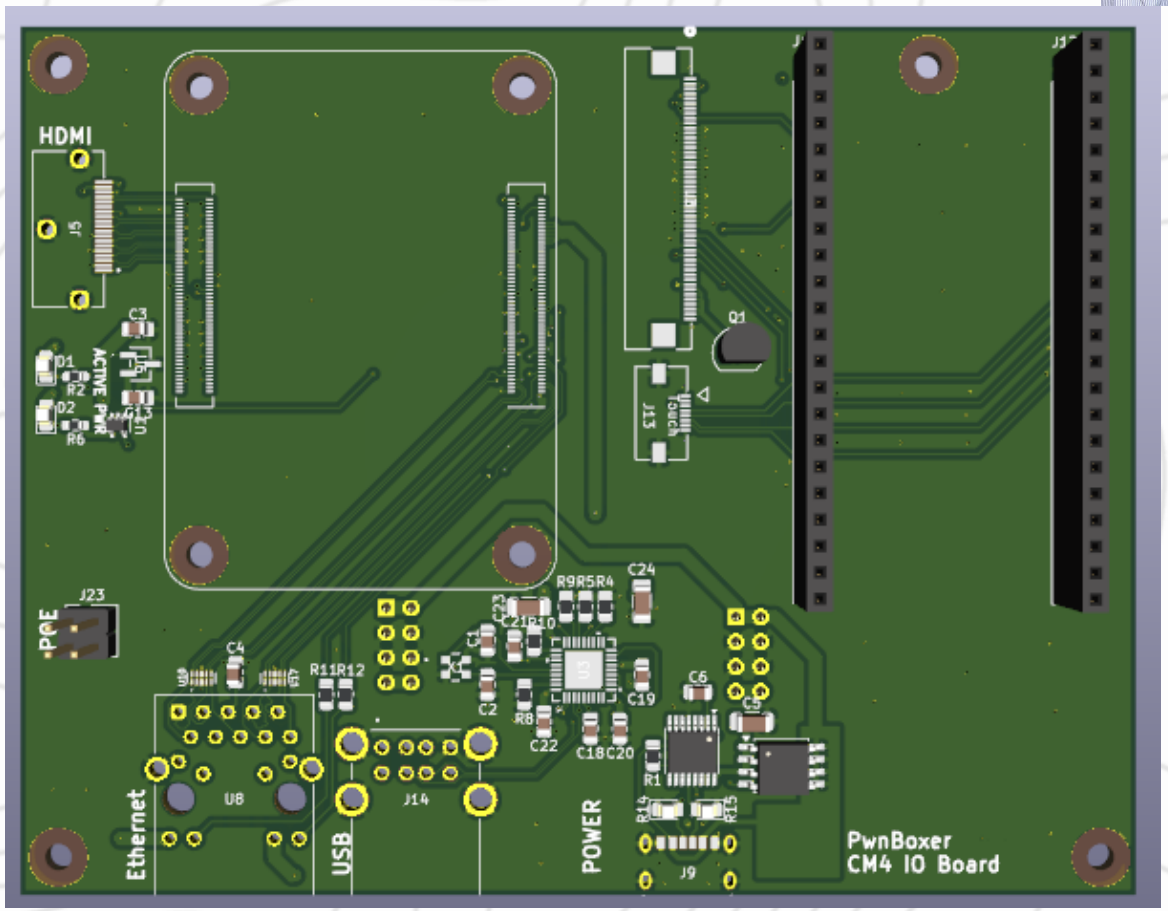
ESP32 Headers &
ZIF Connectors



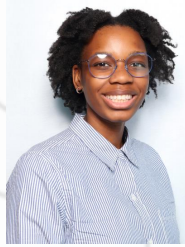
Power

MAIN BOARD PCB DESIGN

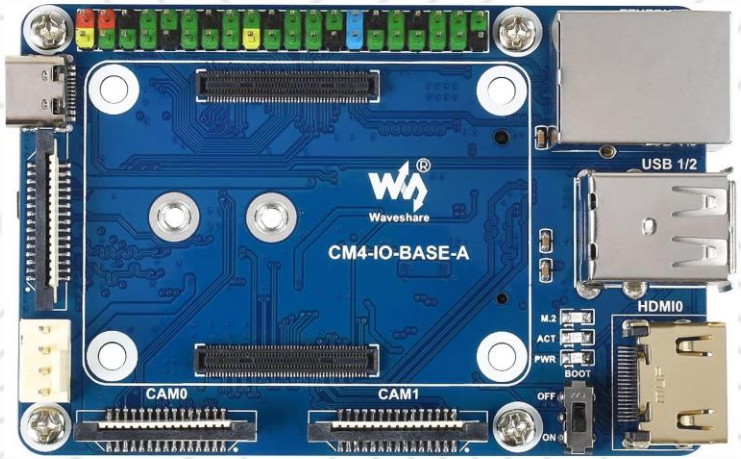




CM4 CARRIER BOARD DESIGN RISK ASSESSMENT



Risk Area	Impact
High Routing Density	PCB layout failure risk, unable to correct in lab
High Speed Design	Signal integrity risk, unable to correct in lab
Layer Count Requirement	$$$, 4 layer boards are expensive
Schedule Impact	Manufacturing dependent delays if board fails

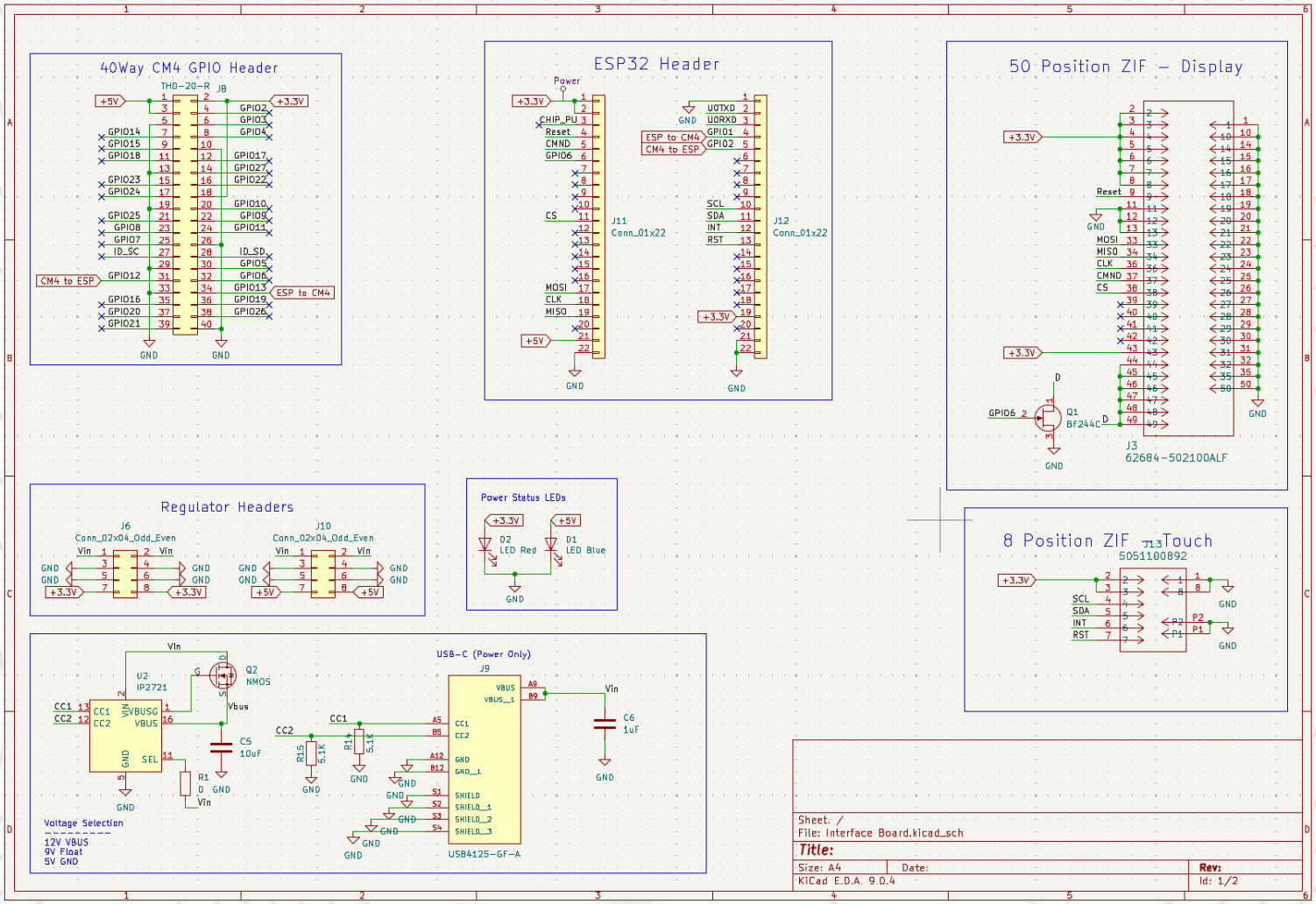


Substitute: Waveshare CM4-IO-BASE-A

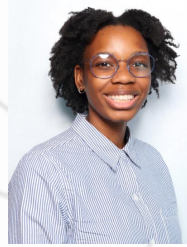
- Small footprint
- Integrated support for all required peripherals
- Pre-validated
- $26.87

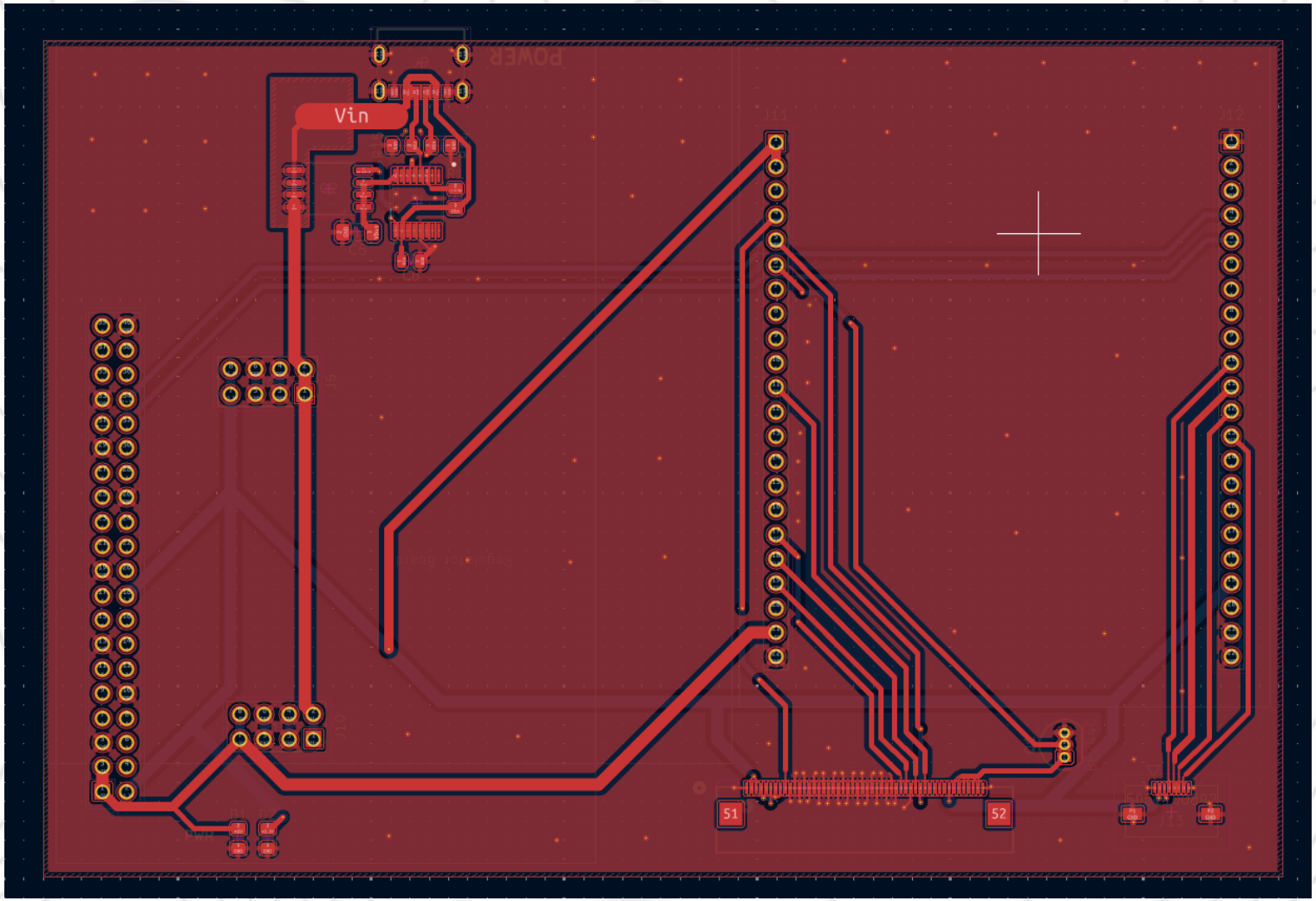
PWNBOXER

MAIN BOARD SCHEMATIC V2



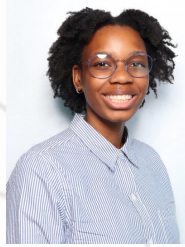
MAIN BOARD PCB DESIGN V2





ESP32 Header

HARDWARE POWER TESTING



Goal: Verify system power consumption under worst-case load and ensure compliance with 15W system limit.

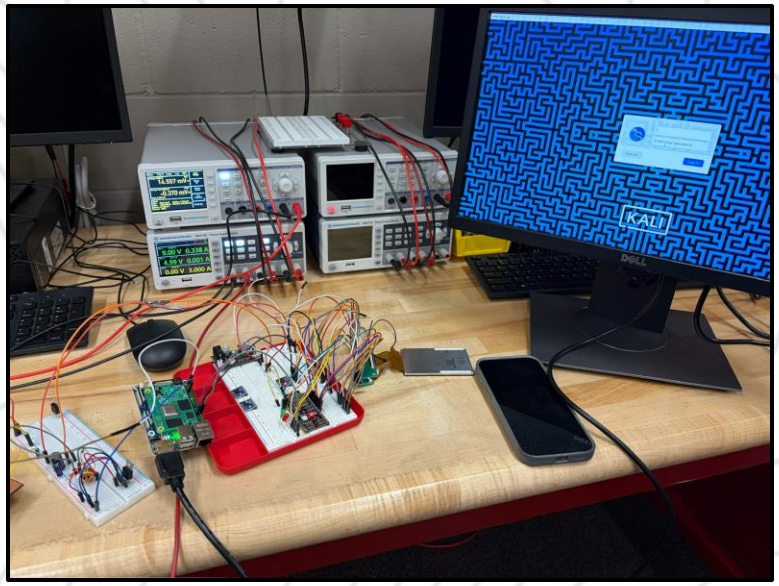
Test Setup

- Breadboard prototype of core system
- Bench supply of 9V
- Regulators connected as in final design
- System run under high workload
- Input current measured

Results

Measured peak current: ≈.8 A

Calculated Power: **7.2 W**



WEBSITE PROTOTYPING AND TESTING

Functional Testing

- User authentication flow validated (registration + login)
- RBAC enforced (admin routes protected)
- Device API-key authentication validated
- Cross-user access prevented (403 validation)

Performance Testing

- Manual upload benchmark: ~1.45-2:00 processing (local environment)
- Concurrent uploads validated (parallel requests handled without data mixing)
- Accurate user-to-report mapping: 100%

Edge Case Testing

- Invalid JWT → rejected
- Revoked API key → rejected
- Wrong device secret → rejected
- Report failure → status updated to failed
- Unauthorized report access → blocked (403)

Tested in local containerized environment (Docker-based stack)

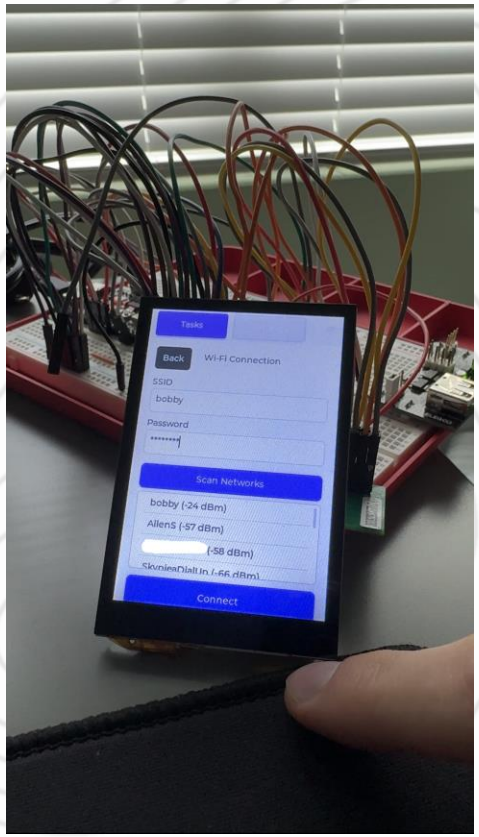
CM4 TOOLING TESTING

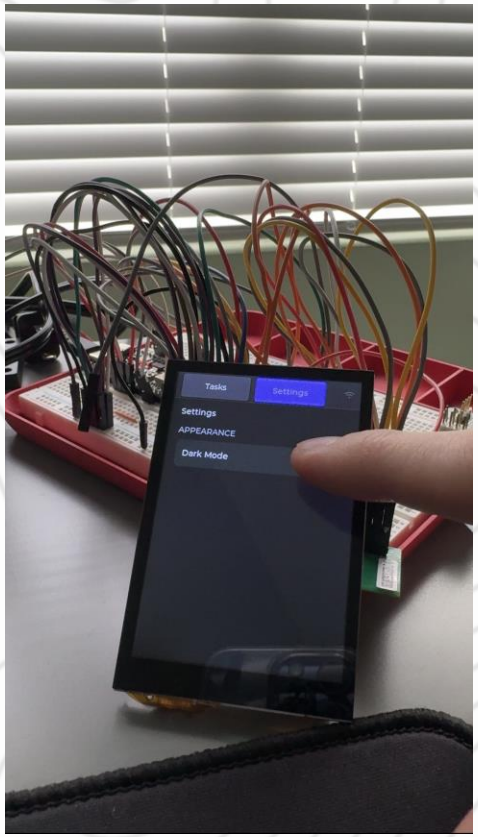
- Testing on the CM4 showed that with direct user intervention, tools ran.
- Manually, tasks can run concurrently with minimal issues.
- Intensive network tasks took significantly longer than on a standard desktop.
- Tools for remote connection are working as expected.

```
Not shown: 65532 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 1000     1000          776 May 30  2021 note.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.100.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
```

UI TESTING

- Built on embedded C++ with LVGL for UI composition/rendering and LovyanGFX for low-level TFT/touch hardware integration
- Uses an LVGL callback functions for navigation, gestures, button actions, text input focus, and on-screen keyboard behavior instead of blocking control flow
- Wi-Fi operations are decoupled from the UI thread via a manager/task boundary to increase performance





PROGRESS/PLAN FOR COMPLETION

Receive PCBs and solder components

Complete GUI software for ESP32 (currently 50%)

Complete networking software for CM4 (currently 30%)

Test completed project and create final demo presentations

BOM

Component	*Part Name*	*Quantity*	*Unit Price*	*Total Price*
Computer Engineer				
Raspberry Pi Compute Module 4	CM4 (8GB RAM, 32GB eMMC, WiFi)	1	$150	$156.38
CM4 IO Board	Waveshare IO Board Lite	1	$35.00	$35.00
Microcontroller	ESP32-S3-WROOM-1	1	$18.99	$18.99
Flash Memory	Winbond 25Q128JVSIQ (16MB SPI Flash)	1	$2.00	$2.00
Display	4.0" TFT LCD w/ Capacitive Touch (SPI, ribbon cable)	1	$45.00	$45.00
USB to UART	CP2102N-A02-GQFN24R	3	$4.14	$12.42
Electrical Engineer				
Custom PCB - Power	OSH Park fabrication (2-layer)	1	$42.40	$42.40
Custom PCB - Main PwnBoxer	OSH Park fabrication (4-layer)	1	$156.90	$156.90
Custom PCB - Interface	OSH Park fabrication (2-layer)	1	$86.20	$86.20
Custom PCB - ESP board	OSH Park fabrication (2-layer)	1	$26.15	$26.15
USB PD	IP2721-MAX12	1	$0.60	$0.60
Pushbutton Switch	SPST tactile button	2	$0.25	$0.50
Power Supply	USB-C Adapter	1	$10.00	$10.00
Stacked USB	72309-7043BLF	1	$2.68	$2.68
Ethernet	1-1734264-1	1	$1.03	$1.03
Miscellaneous	USB hub, wiring, headers, mounting hardware, etc.	–	$136.02	$136.02
Total Cost				
Computer Engineer		$267.79		
Electrical Engineer		$462.48		
Grand Total - Funded entirely by Dr. Mike		**$732.27**		

ADMINISTRATIVE CONTENT – WORKLOAD DISTRIBUTION

Franco Mezzarapa

- CM4 software environment setup and configuration
- ESP32 ↔ Raspberry Pi communication pipeline
- Network scanning integration and device orchestration

Abdiel Marcano

- Full web portal development (frontend + backend)
- API architecture (Node.js / Express)
- Authentication and authorization (JWT, API keys)
- Database design and integration (PostgreSQL + Prisma)
- Report lifecycle + LLM processing pipeline
- System architecture and cloud/web integration

Robert Lee

- TFT display GUI on Raspberry Pi
- Local device interface and user interaction logic
- Display pipeline for scan status and outputs
- On-device usability and control flow

Gugulethu Sigogo

- Custom PCB design and fabrication coordination
- Soldering, board bring-up, and hardware assembly
- Power and connectivity hardware integration
- Electrical validation and debugging

THANK YOU